TFW 2131

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Serial No. : 09/655,229 Confirmation No. 7777
Applicant : Chung Nan Chang
Filed : September 5, 2000
Title : SECURE CRYPTOGRAPHIC KEY EXCHANGE AND VERIFIABLE DIGITAL SIGNATURE
TC/A.U. : 2131
Examiner : Shin-Hon Chen

Docket No. : 2174
Customer No.: 23320

MAIL STOP AMENDMENT
Commissioner for Patents
Post Office Box 1450
Alexandria, Virginia 22313-1450

Sir:

Transmitted herewith is a full and complete response to an Office Action dated December 29, 2005, for the patent application identified above.

Small entity status under 37 C.F.R. §§ 1.9 and 1.27 has been established for this application by a previously submitted verified statement.

Applicant believes that no additional fee is required for filing the amendment set forth in the accompanying response.

Applicant hereby petitions for a one (1) month extension of time in which to respond to the Office Action, and submits a check in the amount of $60.00 in payment of the small entity fee for a one (1) month extension. If any additional extension of time is required to make this response timely, then pursuant to the relevant provision of 37 C.F.R. § 1.136, Applicant hereby conditionally petitions for an extension of time sufficient to make the response timely.

If any additional fee is due, the Commissioner for Patents is hereby authorized to charge any deficiency or credit any surplus in the enclosed fee to Deposit Account No. 19-0735. A duplicate copy of this transmittal letter is enclosed herewith.

Respectfully submitted

Donald E. Schreiber
Reg. No. 29,435

Dated: 1 May, 2006

Donald E. Schreiber
A Professional Corporation
Post Office Box 2926
Kings Beach, CA 96143-2926

Telephone: (530) 546-6041

Attorney for Applicant

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify pursuant to 37 C.F.R. § 1.8(a)(1) that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

MAIL STOP AMENDMENT
Commissioner for Patents
Post Office Box 1450
Alexandria, Virginia 22313-1450

on 1 May, **200**6.

Donald E. Schreiber

Dated: 1 May, **200**6

Donald E. Schreiber
A Professional Corporation
Post Office Box 2926
Kings Beach, CA 96143-2926
(530) 546-6041

Serial No.	: 09/655,229	Confirmation No. 7777
Applicant	: Chung Nan Chang	
Filed	: September 5, 2000	
Title	: SECURE CRYPTOGRAPHIC KEY EXCHANGE AND VERIFIABLE DIGITAL SIGNATURE	
TC/A.U.	: 2131	
Examiner	: Shin-Hon Chen	
Docket No.	: 2174	
Customer No.	: 23320	

MAIL STOP AMENDMENT
Commissioner for Patents
Post Office Box 1450
Alexandria, Virginia 22313-1450

Sir:

This communication responds to an Office Action dated December 29, 2005, for the patent application identified above which, inter alia, contains a non-final rejection of all claims pending in the patent application.

Introductory Remarks

On January 18, 2005, the United States Patent and Trademark Office ("USPTO") mailed an Office Action containing a final rejection of all claims pending in this patent application. On April 18, 2005, Applicant filed a Notice of Appeal of the final rejection of the pending claims followed on June 20, 2005, Applicant by an Appeal Brief.

Paragraphs 23 and 24 of the December 29, 2005, Office Action on pages 12 and 13 thereof declares that:

1. Applicant's arguments with respect to claims 1-29 (apparently appearing the June 20, 2005, Appeal Brief) have been considered moot in view of the new grounds of rejection appearing in the December 29, 2005, Office Action; and
2. the application has been re-opened for prosecution in response to the Appeal Brief filed on June 20, 2005.

The rejection of claims appearing in both Office Actions, i.e. the Office Actions respectively dated January 18, 2005 and December 29, 2005, **rely upon a single reference, i.e. United States Patent No. 5,805,703** entitled "Method and Apparatus for Digital Signature Authentication" which issued September 8, 1998, on an application filed by Richard E. Crandall ("the Crandall patent").

Attached hereto as Exhibit A is a comparison of paragraph 4 appearing in the January 18, 2005, Office Action with paragraphs 5 through 22 appearing in the December 29, 2005, Office Action. The comparison appearing in Exhibit A establishes that, other than for a reformatting of the text of paragraph 4 of the January 18, 2005, Office Action, the rejection of claims appearing in paragraphs 5 through 22 of the pending Office Action are word-for-word identical to those appearing in the prior, January 18, 2005, Office Action except for:

1. paragraph 5 of the December 29, 2005, Office Action which changes the basis for rejecting claims from anticipation under 35 U.S.C. § 102(b) to obviousness under 35 U.S.C. § 103(a);
2. paragraph 6 of the December 29, 2005, Office Action which, with respect to independent claim 1:
   a. deletes an allegation from the January 18, 2005, Office Action that:

      > the receiving unit R transmitting for storage in a publicly accessible repository a plurality of public quantities (Crandall: column 20 lines 15-24 and figure 12: store publicly known information);

   b. **expressly admits that the basis for rejecting independent claim 1 appearing in all prior Office Actions is erroneous**; and

c. replaces the preceding admittedly fallacious allegation with a new allegation that:

> **Crandall does not explicitly disclose the receiving unit R transmitting for storage in a publicly accessible repository a plurality of public quantities**. However, Crandall discloses that the publicly accessible repository contains a plurality of public quantities of receiving unit (Crandall: column 20 lines 15-24 and figure 12: store publicly known information). **It would have been obvious to one having ordinary skill in the art to have the receiving unit transmit the plurality of public quantities to the publicly accessible repository because it enables the sending unit to retrieve information required to send encrypted message to receiving unit**.

3. paragraph 14 of the December 29, 2005, Office Action which, with respect to independent claims 10 and 19:

a. deletes an allegation from the January 18, 2005, Office Action that:

> when the cryptographic unit is to receive the ciphertext message M:
> (1) storing plurality of public quantities in a publicly accessible repository (Crandall: column 20 lines 15-24 and figure 12: store publicly known information);

b. **expressly admits that the basis for rejecting independent claims 10 and 19 appearing in all prior Office Actions is erroneous**; and

c. replaces the preceding admittedly fallacious allegation with a new allegation that:

> **Crandall does not explicitly disclose the receiving unit R transmitting for storage in a publicly accessible repository a plurality of public quantities**. However, Crandall discloses that the publicly accessible repository contains a plurality of public quantities of receiving unit (Crandall: column 20 lines 15-24 and figure 12: store publicly known information). **It would have been obvious to one having ordinary skill in the art to have the receiving unit transmit the plurality of public quantities to the publicly accessible repository because it enables the sending unit to retrieve information required to send encrypted message to receiving unit**; and

4. paragraph 21 of the December 29, 2005, Office Action which, with respect to independent claim 28:

   a. deletes an allegation from the January 18, 2005, Office Action that:

      > the sending unit S transmits for storage in a publicly accessible repository a plurality of public quantities (Crandall: column 20 lines 15-24: store publicly known information);

   b. **expressly admits that the basis for rejecting independent claim 28 appearing in all prior Office Actions is erroneous**; and

   c. replaces the preceding admittedly fallacious allegation with a new allegation that:

      > **Crandall does not explicitly disclose the transmitting unit 5 transmitting for storage in a publicly accessible repository a plurality of public quantities**. However, Crandall discloses that the publicly accessible repository contains a plurality of public quantities of receiving unit (Crandall: column 20 lines

> 15-24 and figure 12: store publicly known information). **It would have been obvious to one having ordinary skill in the art to have the receiving unit transmit the plurality of public quantities to the publicly accessible repository because it enables the sending unit to retrieve information required to send encrypted message to receiving unit**.

Those portions of the December 29, 2006, Office Action rejecting independent claims 1, 10, 19 and 28 excerpted above all rely upon a conclusory allegation that:

> **it would have been obvious to one having ordinary skill in the art to have the receiving unit transmit the plurality of public quantities to the publicly accessible repository** . . . .

Applicant respectfully submits that the Crandall patent in column 7 at lines 30-31 teaches away from the preceding hypothesis in a section of the reference entitled "Elliptic Curve Algebra" where the reference expressly states:

> [n]ext, parameters are established **for** both sender and recipient.

Because the Crandall patent expressly teaches away from the Office Action's hypothesis, Applicant respectfully submits that legal precedents identified below mandate that **a prima facie rejection of the pending claims for obviousness must include a citation to facts appearing in the reference which supports the preceding hypothesis**. Under those controlling legal precedents, anything less than a citation to facts appearing in the reference supporting the

hypothesis constitutes nothing more than a hindsight reconstruction of the application's pending claims.

When as in the present application a single reference is applied in rejecting claims for obviousness under 35 U.S.C. § 103(a), the Court of Appeals for the Federal Circuit in In re Mills, 916 F.2d 680, 682, 16 USPQ2d 1430, 1432 (Fed. Cir. 1990) directs that **although a prior art device "may be capable of being modified to run the way [the inventive] apparatus is claimed, there must be a suggestion or motivation in the reference to do so**." In re Naylor, 369 F.2d 765, 768, 152 USPQ 106, 108 (CCPA 1967) quoting In re Spormann, 363 F.2d 444, 448, 150 USPQ 449, 452 (CCPA 1966). (Emphasis supplied.)

> The motivation, suggestion or teaching may come explicitly from statements in the prior art, the knowledge of one of ordinary skill in the art, or, in some cases the nature of the problem to be solved. See Dembiczak, 175 F.3d at 999, 50 USPQ2d at 1617. In addition, the teaching, motivation or suggestion may be implicit from the prior art as a whole, rather than expressly stated in the references. See WMS Gaming, Inc. v. International Game Tech., 184 F.3d 1339, 1355, 51 USPQ2d 1385, 1397 (Fed. Cir. 1999). **The test for an implicit showing is what the combined teachings, knowledge of one of ordinary skill in the art, and the nature of the problem to be solved as a whole would have suggested to those of ordinary skill in the art**. See In re Keller, 642 F.2d 413, 425, 208 USPQ 871, 881 (CCPA 1981) (and cases cited therein). **Whether the Board relies on an express or an implicit showing, it must provide particular findings related thereto**. See Dembiczak, 175 F.3d at 999, 50 USPQ2d at 1617. **Broad conclusory statements standing alone are not "evidence**." Id. In Re Werner Kotzab, 217 F.3d 1365, 1369, 55 USPQ2d 1313, 1316 (Fed. Cir. 2000). (Emphasis supplied.)

Since the rejections of independent claims 1, 10, 19 and 28 in the December 29, 2005, Office Action fail to identify any facts in the reference, i.e. the Crandall patent, which supports the Office Action's broad conclusory statements excerpted above, Applicant respectfully:

1. submits that the December 29, 2005, Office Action fails to establish a prima facie obviousness rejection;
2. requests that the rejection be withdrawn; and
3. requests that this patent application pass promptly to issue.

AMENDMENTS

There are no **Amendments to the Specification.**

The Listing of Claims, which begins on page 10 of this Response, contains no **Amendments to the Claims** as originally filed on September 5, 2000.

There are no **Amendments to the Drawings.**

Remarks/Arguments begin on page 24 of this Response.